HEALTH AFFAIRS

TRICARE

TRICARE
Management
Activity

HIPAA Security Topics

Web Resources, Implementation Guide and Biomedical Devices

HIPAA Training 2006

TMA Privacy Office

This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.

Agenda

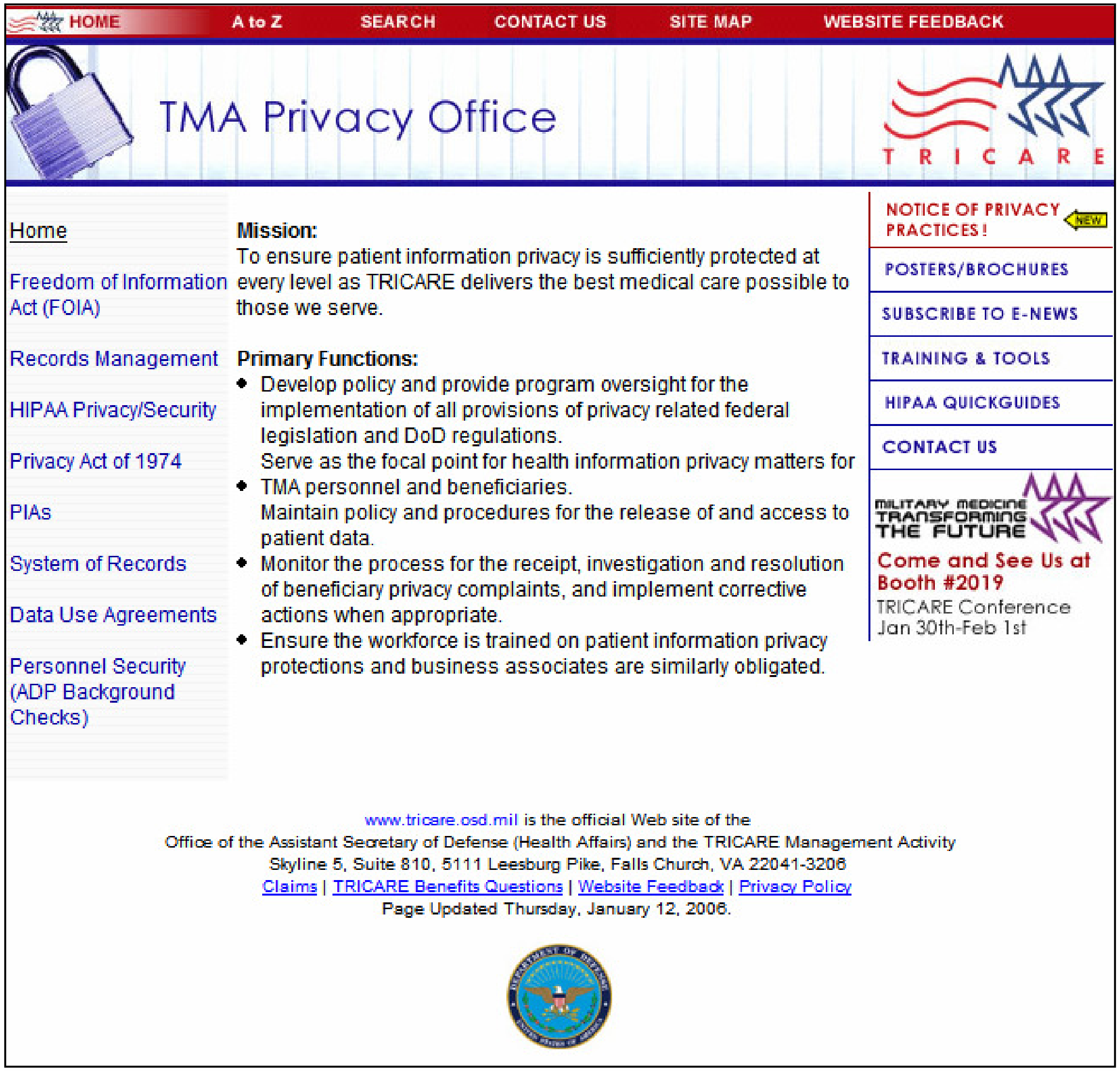
- TMA Privacy Office HIPAA Security Web Site
- Risk Information Management Resource (RIMR)
- HIPAA Security Implementation Guide
- HIPAA Security and Biomedical Devices

Training Objectives

- Upon completion of this course you will be able to:
  - Identify available resources to aide in security awareness
  - Identify available training briefings
  - Identify available resources to aide in implementation of HIPAA security
  - Describe the relationship between HIPAA security and biomedical devices

TMA Privacy Office
HIPAA Security Web Site

TMA HIPAA Security Web Site
http://www.tricare.osd.mil/tmaprivacy
(1 of 2)



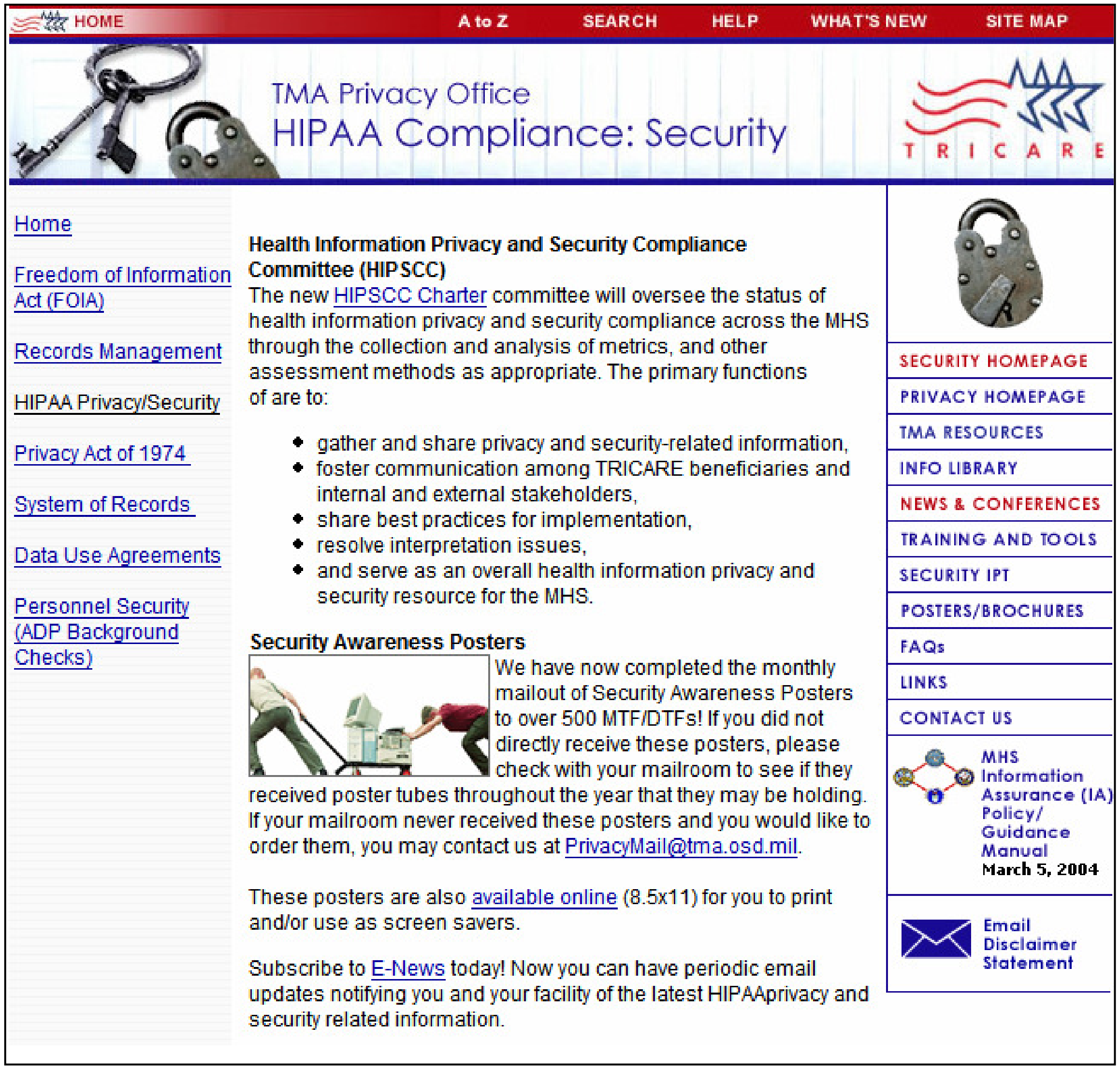
Mission:
To ensure patient information privacy is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

Primary Functions:

- Develop policy and provide program oversight for the implementation of all provisions of privacy related federal legislation and DoD regulations.
- Serve as the focal point for health information privacy matters for TMA personnel and beneficiaries.
- Maintain policy and procedures for the release of and access to patient data.
- Monitor the process for the receipt, investigation and resolution of beneficiary privacy complaints, and implement corrective actions when appropriate.
- Ensure the workforce is trained on patient information privacy protections and business associates are similarly obligated.

www.tricare.osd.mil is the official Web site of the
Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity
Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Claims | TRICARE Benefits Questions | Website Feedback | Privacy Policy
Page Updated Thursday, January 12, 2006.

TMA HIPAA Security Web Site
http://www.tricare.osd.mil/tmaprivacy
(2 of 2)



Health Information Privacy and Security Compliance Committee (HIPSCC)

The new HIPSCC Charter committee will oversee the status of health information privacy and security compliance across the MHS through the collection and analysis of metrics, and other assessment methods as appropriate. The primary functions of are to:

- gather and share privacy and security-related information,
- foster communication among TRICARE beneficiaries and internal and external stakeholders,
- share best practices for implementation,
- resolve interpretation issues,
- and serve as an overall health information privacy and security resource for the MHS.

Security Awareness Posters

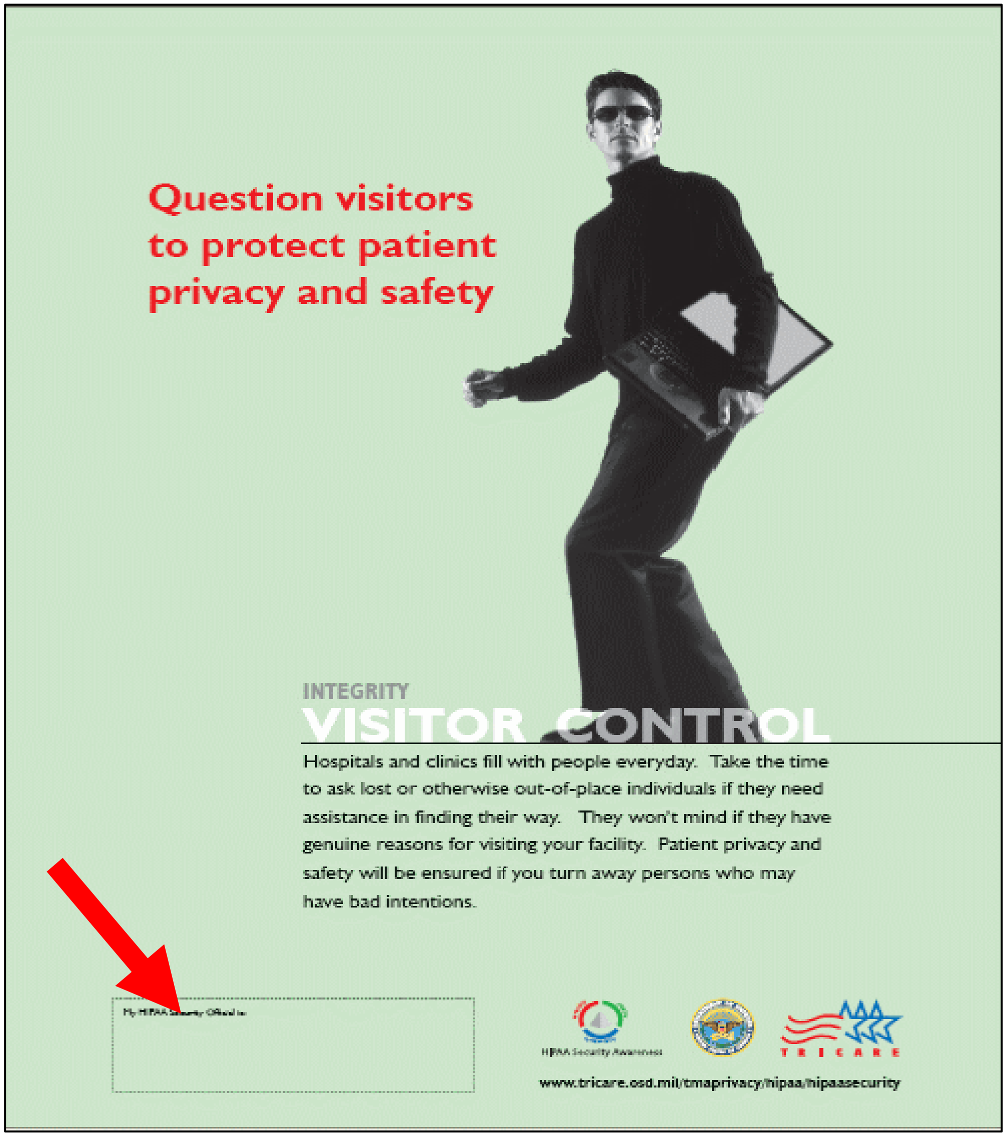
We have now completed the monthly mailout of Security Awareness Posters to over 500 MTF/DTFs! If you did not directly receive these posters, please check with your mailroom to see if they received poster tubes throughout the year that they may be holding. If your mailroom never received these posters and you would like to order them, you may contact us at PrivacyMail@tma.osd.mil.

These posters are also available online (8.5x11) for you to print and/or use as screen savers.

Subscribe to E-News today! Now you can have periodic email updates notifying you and your facility of the latest HIPAAprivacy and security related information.

TMA HIPAA Security Web Site

HIPAA Security Poster Campaign (1 of 2)



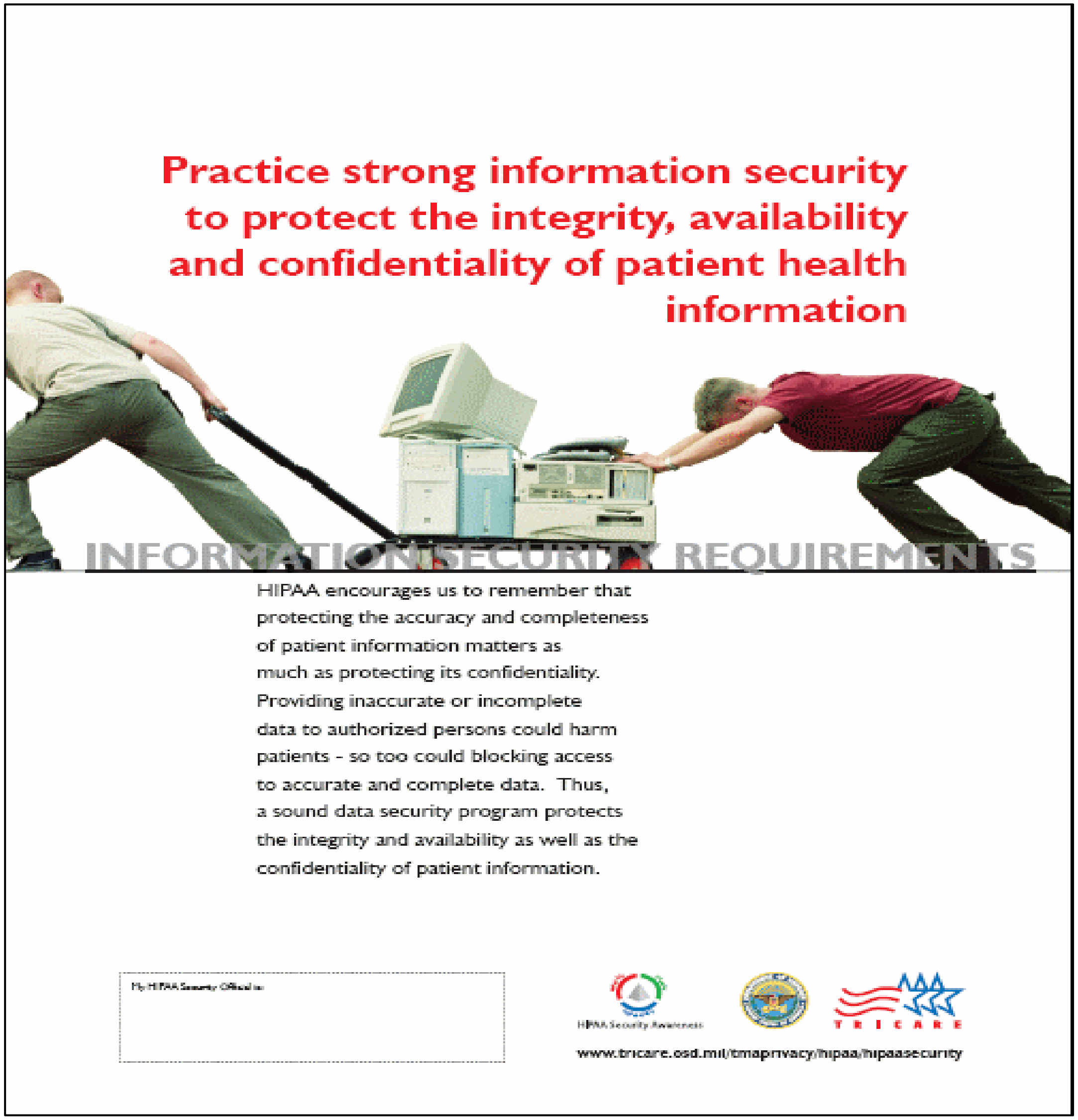
Hospitals and clinics fill with people everyday. Take the time to ask lost or otherwise out-of-place individuals if they need assistance in finding their way. They won't mind if they have genuine reasons for visiting your facility. Patient privacy and safety will be ensured if you turn away persons who may have bad intentions.

My HIPAA Security Official is:

www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

TMA HIPAA Security Web Site

HIPAA Security Poster Campaign (2 of 2)



Practice strong information security to protect the integrity, availability and confidentiality of patient health information

INFORMATION SECURITY REQUIREMENTS

HIPAA encourages us to remember that protecting the accuracy and completeness of patient information matters as much as protecting its confidentiality. Providing inaccurate or incomplete data to authorized persons could harm patients - so too could blocking access to accurate and complete data. Thus, a sound data security program protects the integrity and availability as well as the confidentiality of patient information.

My HIPAA Security Official is:

HIPAA Security Awareness

TRICARE

www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

TMA HIPAA Security Web Site

Summary

- You should now be able to:
  - Locate information pertaining to security topics and HIPAA security management
  - Locate information pertaining to HIPAA support tools and training
  - Locate information pertaining to HIPAA news, conferences and e-news

Risk Information Management Resource (RIMR)

RIMR

Objectives

- Upon completion of this lesson, you should be able to:
  - Identify what systems and processes form RIMR
  - Describe the information the database stores and provides
  - Identify who developed the RIMR and how it helps you maintain compliancy

What is RIMR?

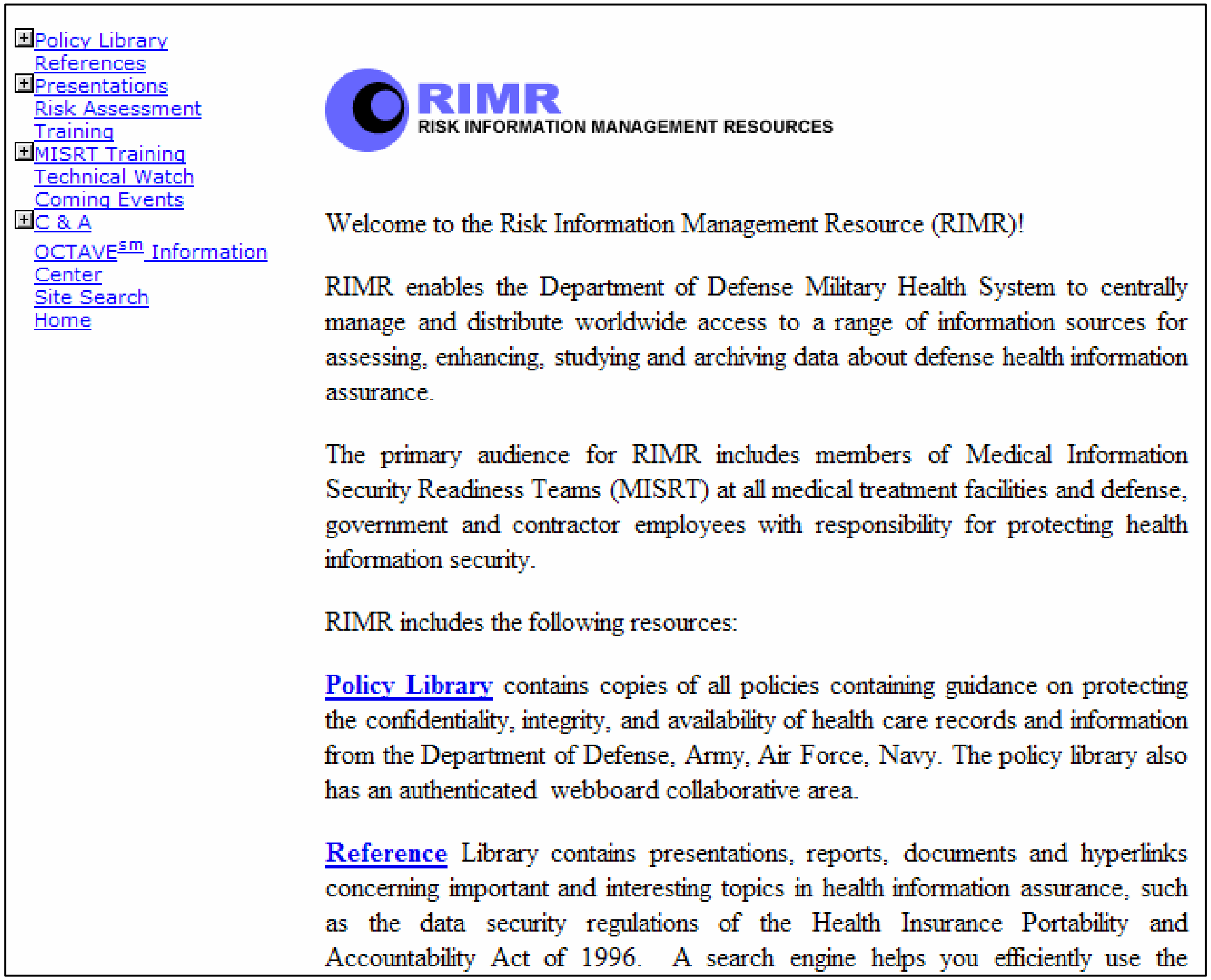
- Web portal provides access to:
  - Information Assurance (IA) resources (policies, case studies, white papers)
  - Plans, Policies and Procedures Working Group (P3WG) HIPAA Privacy and Security Reports
  - Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE^{SM}) (including methodology, automated tool, risk database and support center)
- Risk Database
  - Stores completed risk assessments
  - Provides aggregate reports
  - Trend analysis
  - Supports enterprise wide problem solving and mitigation

Who Developed RIMR

- Congressionally funded through Defense Health Information Assurance Program (DHIAP)
- Currently located at Ft. Detrick
- DoD owned – not vender owned
- Developers
  - Advanced Technology Institute, Charleston SC
  - KRM Associates, Inc, Shepherdstown WV
  - Software Engineering Institute at Carnegie Mellon (CERT), Pittsburgh PA

RIMR

Where is RIMR? - http://rimr.tatrc.org



- ⊞ Policy Library
- References
- ⊞ Presentations
- Risk Assessment
- Training
- ⊞ MISRT Training
- Technical Watch
- Coming Events
- ⊞ C & A
- OCTAVE^{sm} Information Center
- Site Search
- Home

RIMR
RISK INFORMATION MANAGEMENT RESOURCES

Welcome to the Risk Information Management Resource (RIMR)!

RIMR enables the Department of Defense Military Health System to centrally manage and distribute worldwide access to a range of information sources for assessing, enhancing, studying and archiving data about defense health information assurance.

The primary audience for RIMR includes members of Medical Information Security Readiness Teams (MISRT) at all medical treatment facilities and defense, government and contractor employees with responsibility for protecting health information security.

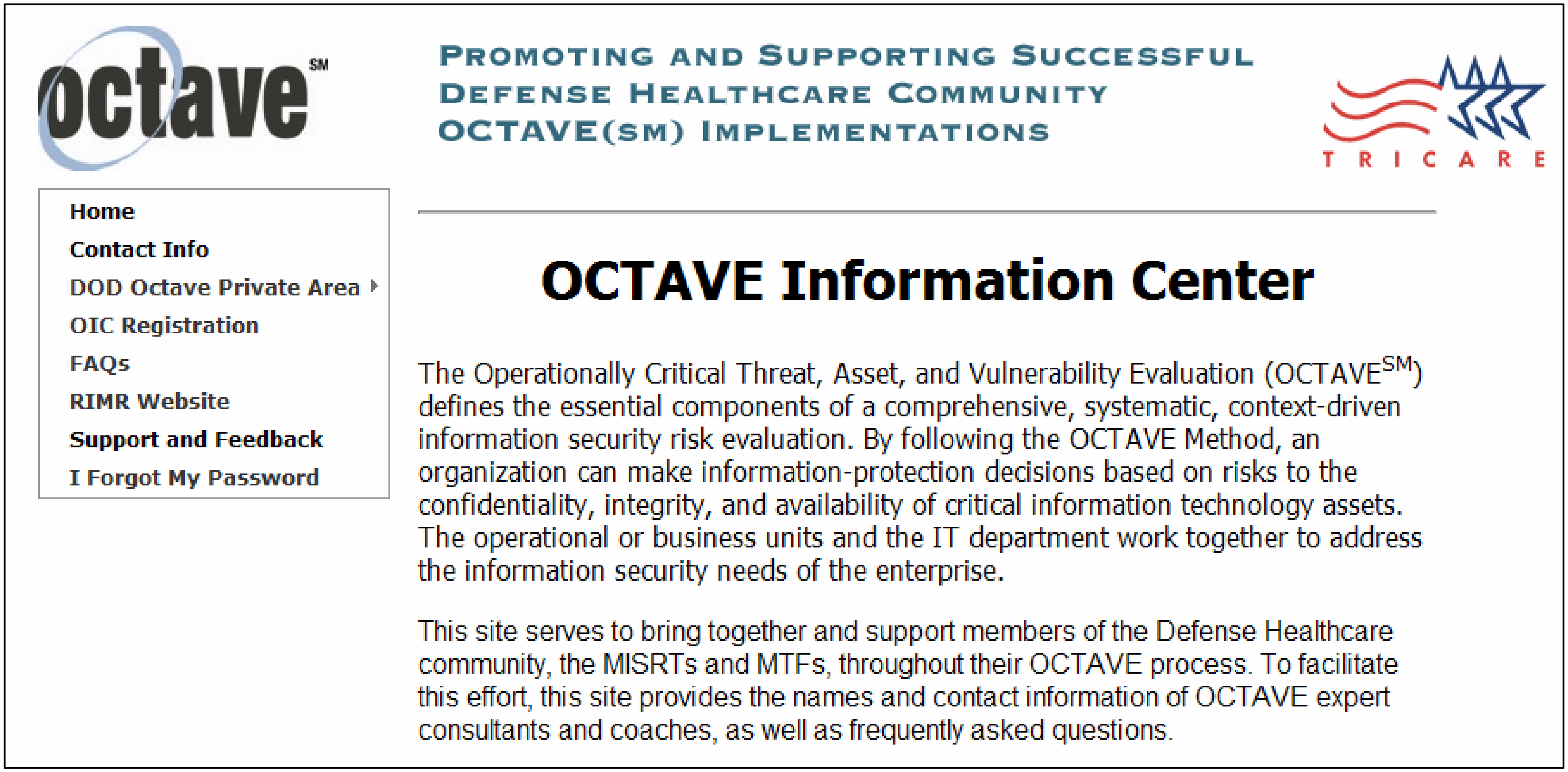
RIMR includes the following resources:

Policy Library contains copies of all policies containing guidance on protecting the confidentiality, integrity, and availability of health care records and information from the Department of Defense, Army, Air Force, Navy. The policy library also has an authenticated webboard collaborative area.

Reference Library contains presentations, reports, documents and hyperlinks concerning important and interesting topics in health information assurance, such as the data security regulations of the Health Insurance Portability and Accountability Act of 1996. A search engine helps you efficiently use the

RIMR

OCTAVE Information Center – New!



OCTAVE Information Center

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM}) defines the essential components of a comprehensive, systematic, context-driven information security risk evaluation. By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets. The operational or business units and the IT department work together to address the information security needs of the enterprise.

This site serves to bring together and support members of the Defense Healthcare community, the MISRTs and MTFs, throughout their OCTAVE process. To facilitate this effort, this site provides the names and contact information of OCTAVE expert consultants and coaches, as well as frequently asked questions.

RIMR

P3WG Final Report Background

- DHIAP and the DoD/HA HIPAA Overarching Integrated Process Team (OIPT) sponsored the formation of the interdisciplinary and inter-service Policies, Procedures, and Practices Workgroup
- Compared all pertinent DoD and service level regulations with the HIPAA Data Security Rule
- Identified gaps and discrepancies and made recommendations for changes

RIMR

Summary

- You should now be able to:
  - Identify what systems and processes form RIMR
  - Describe the information the database stores and provides
  - Identify who developed the RIMR and how it helps you maintain compliancy

HIPAA Security Implementation Guide

HIPAA Security Implementation Guide

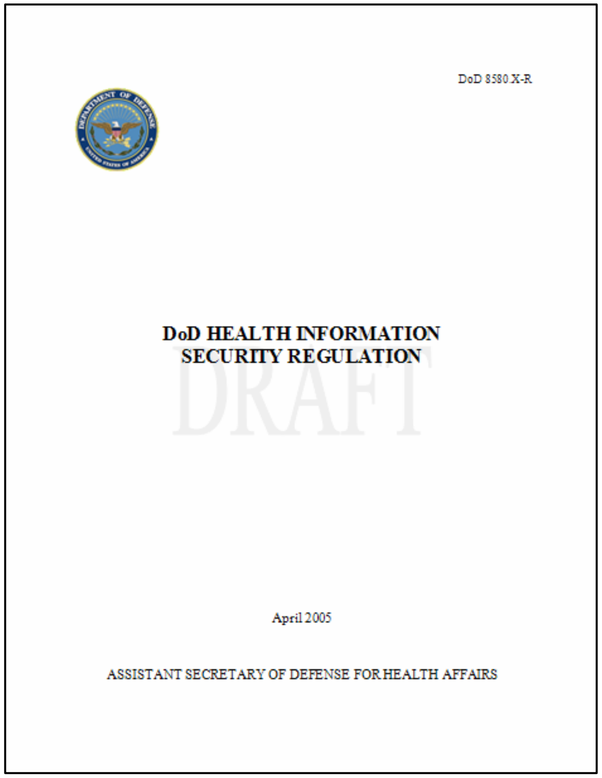
Objectives

- Upon completion of this lesson, you should be able to:
  - Identify the purpose and organization of the Implementation Guide

HIPAA Security Implementation Guide

Purpose (1 of 2)

- Provide guidance with the implementation of
  - DoD 8580.X-R, DoD Health Information Security Regulation



DoD 8580.X-R

DoD HEALTH INFORMATION SECURITY REGULATION

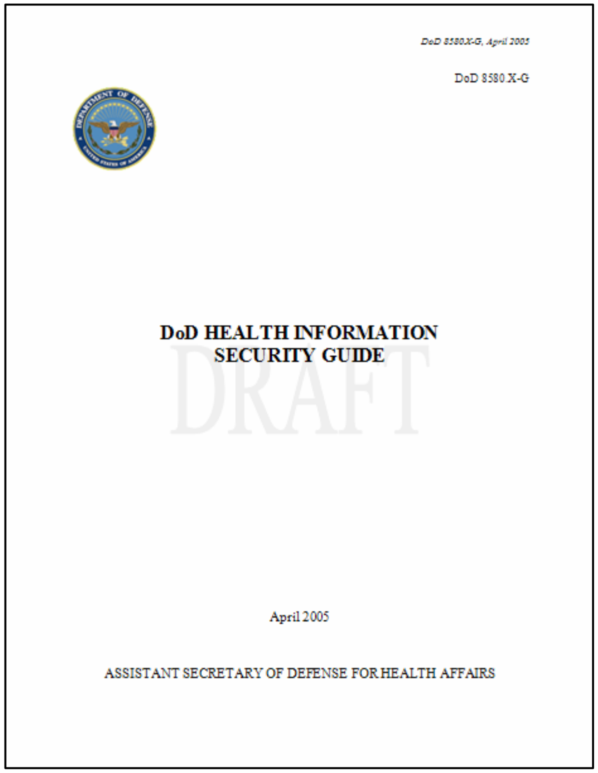
April 2005

ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS

HIPAA Security Implementation Guide

Purpose (2 of 2)

- Contains “actionable steps” towards compliance



DoD 8580.X-G, April 2005

DoD 8580.X-G

DoD HEALTH INFORMATION
SECURITY GUIDE

April 2005

ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS

HIPAA Security Implementation Guide

Organization of Guide (1 of 3)

- Chapter 1: General Information
  - Background
    - History of HIPAA
  - What is HIPAA Security
    - Definition
    - Key concepts and terms
    - Organization of requirements within the security rule
  - Compliance
    - How to achieve HIPAA Security compliance

HIPAA Security Implementation Guide

Organization of Guide (2 of 3)

- Chapter 1: General Information (cont.)
  - Existing DoD Requirements
    - Explanation of why most HIPAA security standards and implementation specifications are required and not addressable
- Chapter 2: Administrative Safeguards
  - Administrative standards and implementation specifications with general guidance on how to achieve compliance
- Chapter 3: Physical Safeguards
  - Physical standards and implementation specifications with general guidance on how to achieve compliance

HIPAA Security Implementation Guide

Organization of Guide (3 of 3)

- Chapter 4: Technical Safeguards
  - Technical standards and implementation specifications with general guidance on how to achieve compliance
- Chapter 5: Policies and Procedures, and Documentation
  - Policies and Procedures, and Documentation standards and implementation specifications with general guidance on how to achieve compliance

Organization of Standards (1 of 4)

- C2.2. ASSIGNED SECURITY RESPONSIBILITY

The number and type of personnel required to implement an organization's security policies in a manner consistent with reference (e) depends on the size and structure of the organization. Document and validate the actual workforce numbers with a breakdown of responsibilities as part of the security management process. The HIPAA Security Regulation states the following:

HIPAA Security Implementation Guide

Organization of Standards (2 of 4)

- C2.2.1. Policy - Identify and assign in writing the security official for the organization who is responsible for the development and implementation of the policies and procedures required by this Regulation. While more than one individual may be given security responsibilities, a single individual must be designated as having the overall final responsibility.

- C2.2.2. Guidance

  - C2.2.2.1. Step 1: Security Official - Select a security official. The ideal candidate should demonstrate competency in the following areas:

HIPAA Security Implementation Guide

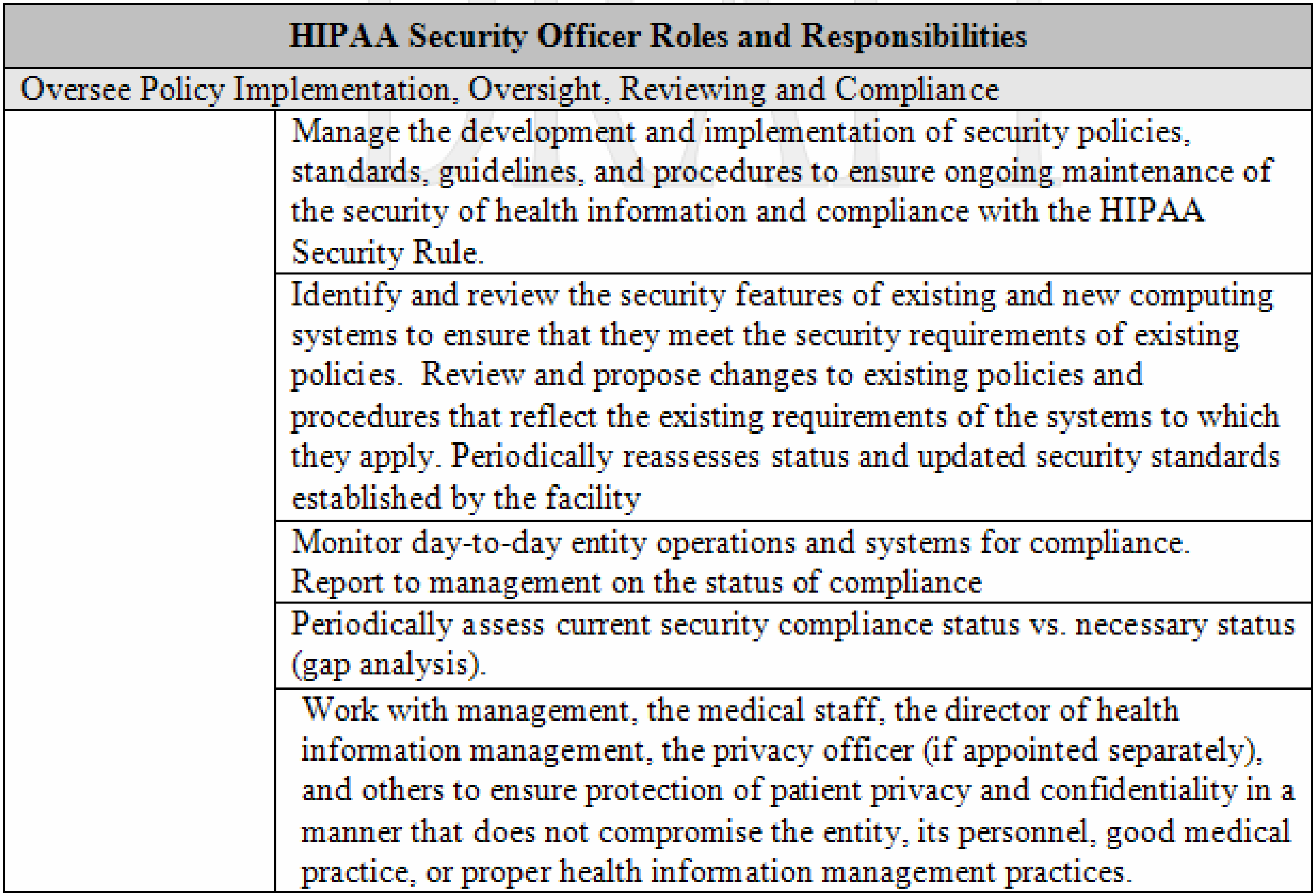
Organization of Standards (3 of 4)

  - C2.2.2.1.1. Ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel
  - C2.2.2.1.2. General understanding of hardware and software security, as well as physical security.
  - C2.2.2.1.3. Familiarity with the legal requirements relating to security and health care operations

- C2.2.2.1. Step 2 - Roles and responsibilities. Assign roles and responsibilities. Table C2.T6. below is a general description of Security Officer roles and responsibilities.

HIPAA Security Implementation Guide

Organization of Standards (4 of 4)

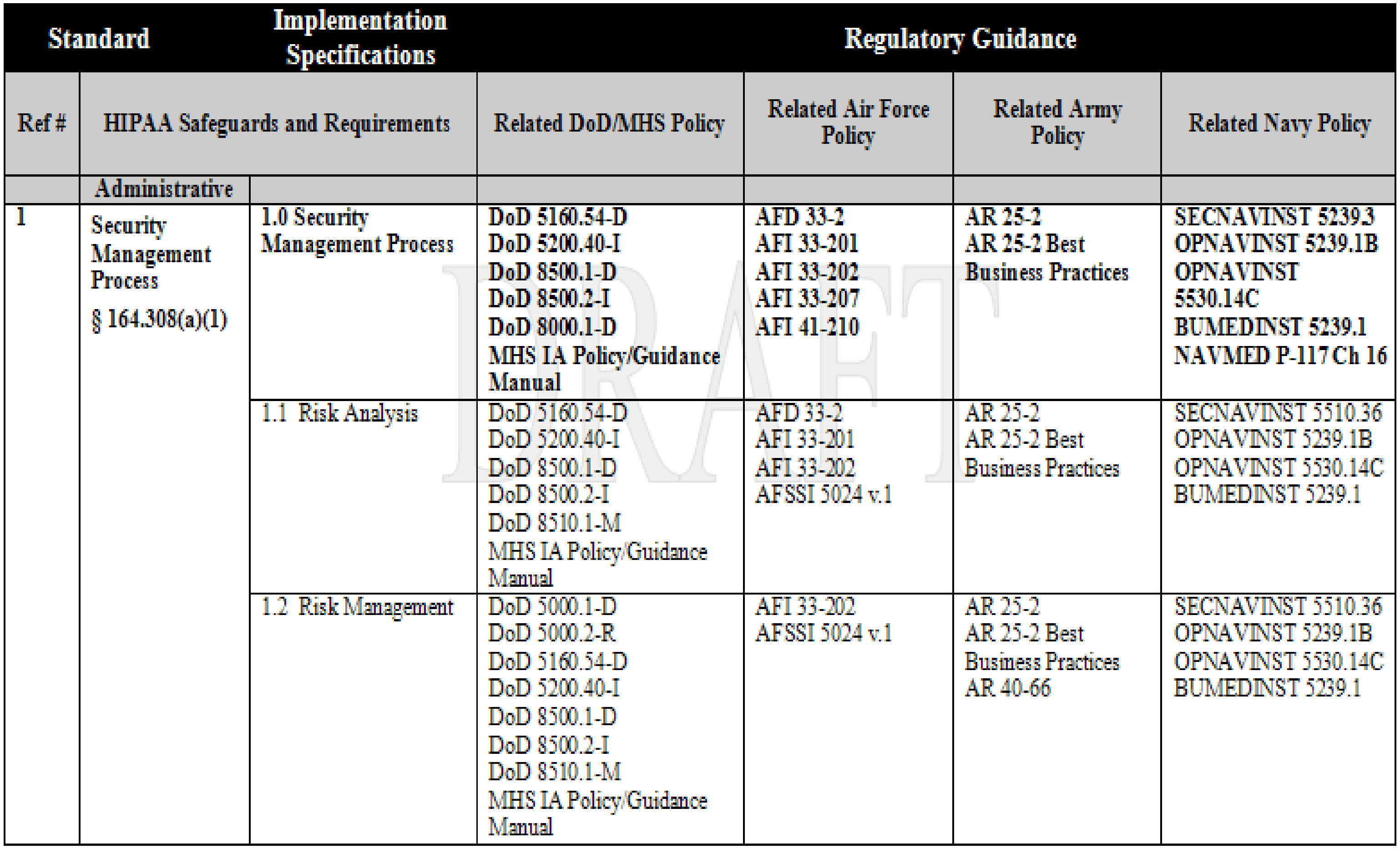


HIPAA Security Officer Roles and Responsibilities	
Oversee Policy Implementation, Oversight, Reviewing and Compliance	
	Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule.
	Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassesses status and updated security standards established by the facility
	Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance
	Periodically assess current security compliance status vs. necessary status (gap analysis).
	Work with management, the medical staff, the director of health information management, the privacy officer (if appointed separately), and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices.

HIPAA Security Implementation Guide

Appendix 1 (1 of 3)

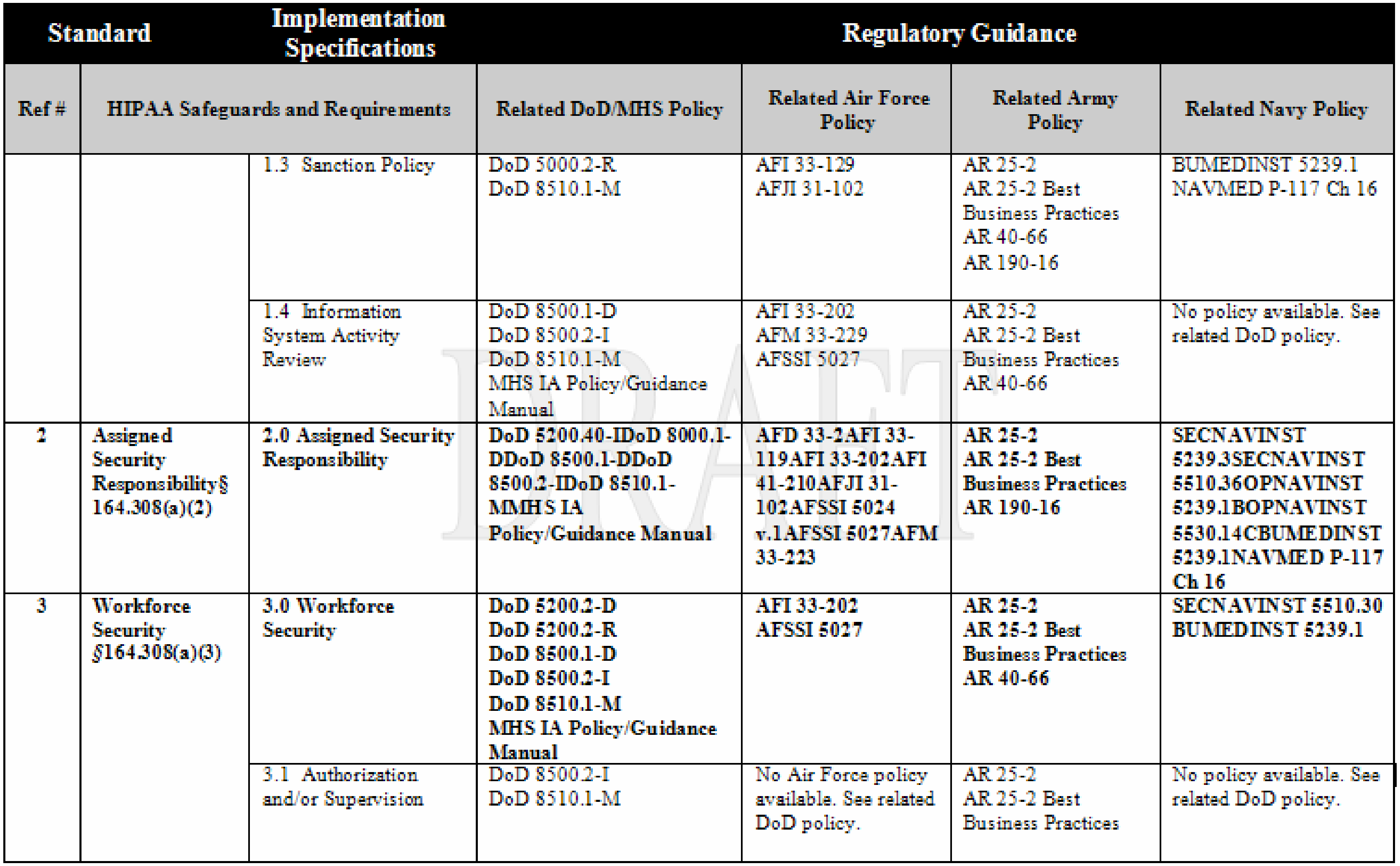
- Appendix 1: Crosswalk of HIPAA to DoD Regulations



Standard		Implementation Specifications	Regulatory Guidance			
Ref #	HIPAA Safeguards and Requirements		Related DoD/MHS Policy	Related Air Force Policy	Related Army Policy	Related Navy Policy
	Administrative					
1	Security Management Process § 164.308(a)(1)	1.0 Security Management Process	DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8000.1-D MHS IA Policy/Guidance Manual	AFD 33-2 AFI 33-201 AFI 33-202 AFI 33-207 AFI 41-210	AR 25-2 AR 25-2 Best Business Practices	SECNAVINST 5239.3 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1 NAVMED P-117 Ch 16
		1.1 Risk Analysis	DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual	AFD 33-2 AFI 33-201 AFI 33-202 AFSSI 5024 v.1	AR 25-2 AR 25-2 Best Business Practices	SECNAVINST 5510.36 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1
		1.2 Risk Management	DoD 5000.1-D DoD 5000.2-R DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual	AFI 33-202 AFSSI 5024 v.1	AR 25-2 AR 25-2 Best Business Practices AR 40-66	SECNAVINST 5510.36 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1

HIPAA Security Implementation Guide

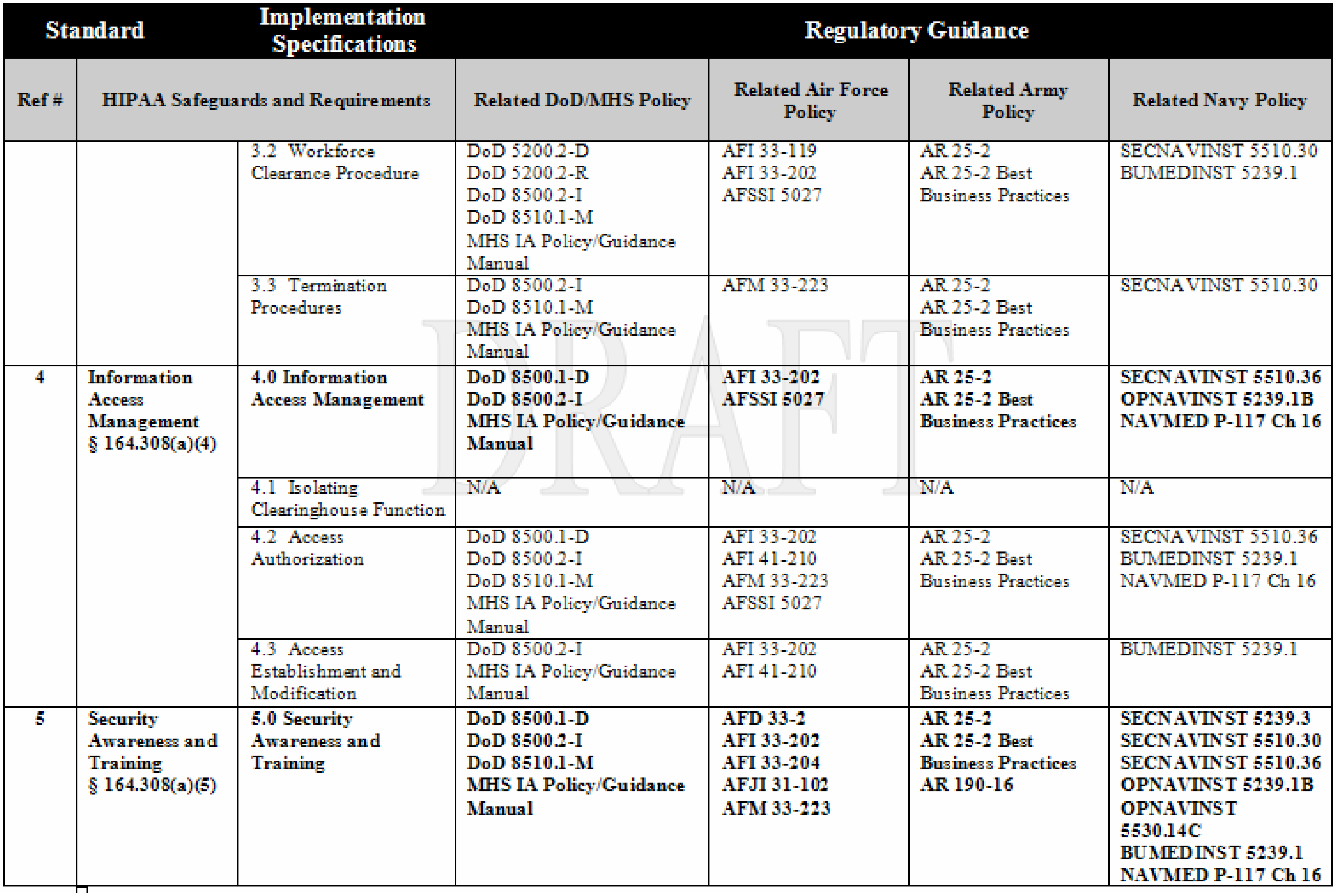
Appendix 1 (2 of 3)



Standard		Implementation Specifications	Regulatory Guidance			
Ref #	HIPAA Safeguards and Requirements		Related DoD/MHS Policy	Related Air Force Policy	Related Army Policy	Related Navy Policy
		1.3 Sanction Policy	DoD 5000.2-R DoD 8510.1-M	AFI 33-129 AFJI 31-102	AR 25-2 AR 25-2 Best Business Practices AR 40-66 AR 190-16	BUMEDINST 5239.1 NAVMED P-117 Ch 16
		1.4 Information System Activity Review	DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual	AFI 33-202 AFM 33-229 AFSSI 5027	AR 25-2 AR 25-2 Best Business Practices AR 40-66	No policy available. See related DoD policy.
2	**Assigned Security Responsibility§ 164.308(a)(2)**	**2.0 Assigned Security Responsibility**	**DoD 5200.40-IDoD 8000.1-DDoD 8500.1-DDoD 8500.2-IDoD 8510.1-MMHS IA Policy/Guidance Manual**	**AFD 33-2AFI 33-119AFI 33-202AFI 41-210AFJI 31-102AFSSI 5024 v.1AFSSI 5027AFM 33-223**	**AR 25-2 AR 25-2 Best Business Practices AR 190-16**	**SECNAVINST 5239.3SECNAVINST 5510.36OPNAVINST 5239.1BOPNAVINST 5530.14CBUMEDINST 5239.1NAVMED P-117 Ch 16**
3	**Workforce Security §164.308(a)(3)**	**3.0 Workforce Security**	**DoD 5200.2-D DoD 5200.2-R DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual**	**AFI 33-202 AFSSI 5027**	**AR 25-2 AR 25-2 Best Business Practices AR 40-66**	**SECNAVINST 5510.30 BUMEDINST 5239.1**
		3.1 Authorization and/or Supervision	DoD 8500.2-I DoD 8510.1-M	No Air Force policy available. See related DoD policy.	AR 25-2 AR 25-2 Best Business Practices	No policy available. See related DoD policy.

HIPAA Security Implementation Guide

Appendix 1 (3 of 3)



Standard		Implementation Specifications	Regulatory Guidance			
Ref #	HIPAA Safeguards and Requirements		Related DoD/MHS Policy	Related Air Force Policy	Related Army Policy	Related Navy Policy
		3.2 Workforce Clearance Procedure	DoD 5200.2-D DoD 5200.2-R DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual	AFI 33-119 AFI 33-202 AFSSI 5027	AR 25-2 AR 25-2 Best Business Practices	SECNAVINST 5510.30 BUMEDINST 5239.1
		3.3 Termination Procedures	DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual	AFM 33-223	AR 25-2 AR 25-2 Best Business Practices	SECNAVINST 5510.30
4	**Information Access Management § 164.308(a)(4)**	**4.0 Information Access Management**	**DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual**	**AFI 33-202 AFSSI 5027**	**AR 25-2 AR 25-2 Best Business Practices**	**SECNAVINST 5510.36 OPNAVINST 5239.1B NAVMED P-117 Ch 16**
		4.1 Isolating Clearinghouse Function	N/A	N/A	N/A	N/A
		4.2 Access Authorization	DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual	AFI 33-202 AFI 41-210 AFM 33-223 AFSSI 5027	AR 25-2 AR 25-2 Best Business Practices	SECNAVINST 5510.36 BUMEDINST 5239.1 NAVMED P-117 Ch 16
		4.3 Access Establishment and Modification	DoD 8500.2-I MHS IA Policy/Guidance Manual	AFI 33-202 AFI 41-210	AR 25-2 AR 25-2 Best Business Practices	BUMEDINST 5239.1
5	**Security Awareness and Training § 164.308(a)(5)**	**5.0 Security Awareness and Training**	**DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual**	**AFD 33-2 AFI 33-202 AFI 33-204 AFJI 31-102 AFM 33-223**	**AR 25-2 AR 25-2 Best Business Practices AR 190-16**	**SECNAVINST 5239.3 SECNAVINST 5510.30 SECNAVINST 5510.36 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1 NAVMED P-117 Ch 16**

HIPAA Security Implementation Guide

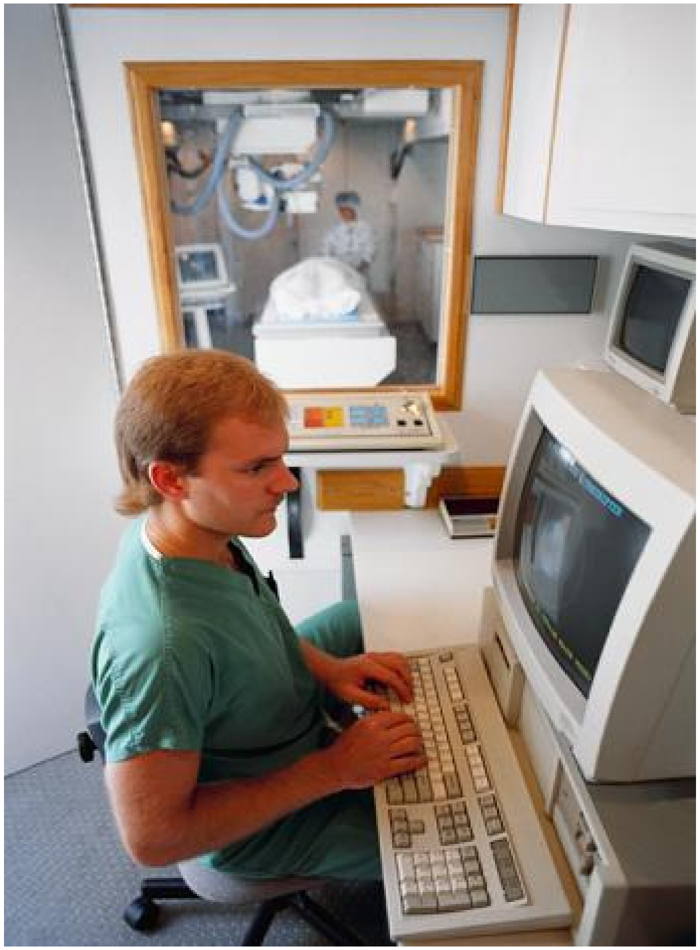
Summary

- You should now be able to:
  - Identify the purpose and organization of the Implementation Guide

HIPAA Security and Biomedical Devices

HIPAA Security and Biomedical Devices

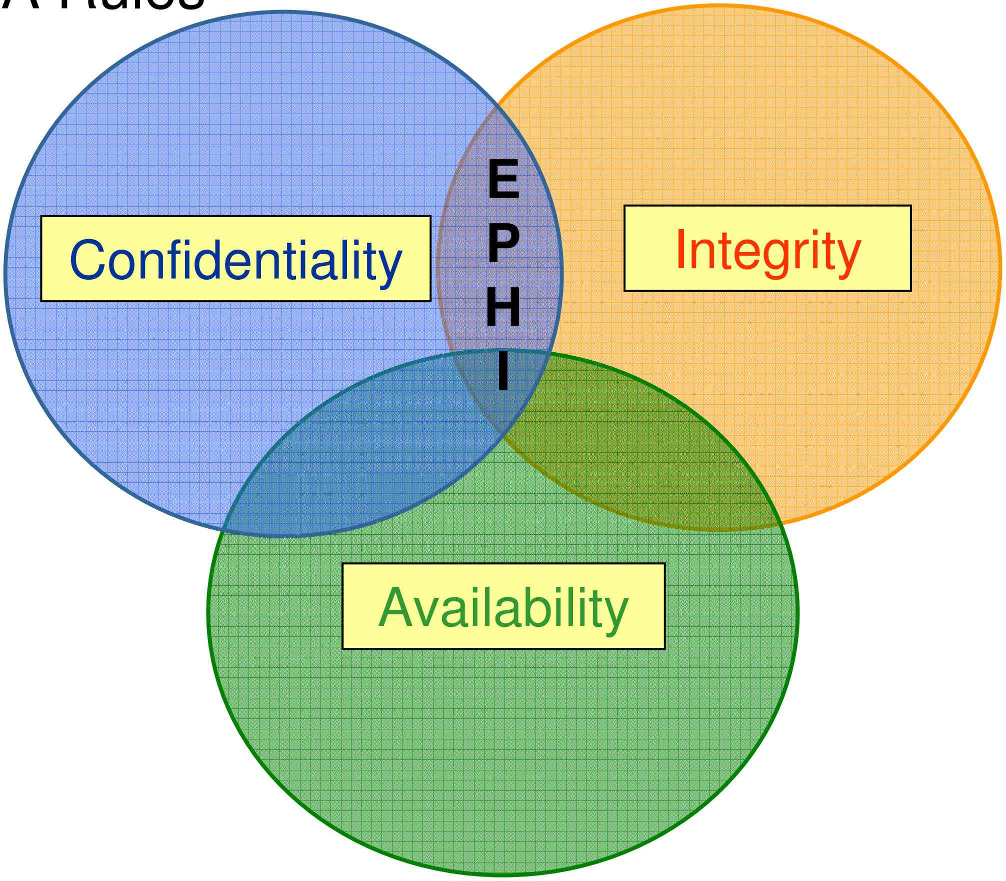
Objectives



- Upon completion of this lesson, you should be able to:
  - Describe the relationship between HIPAA security and biomedical devices
  - Detail the risks of using biomedical devices
  - Identify approaches for minimizing these vulnerabilities

HIPAA Security Requirement

- Must protect the confidentiality, integrity, and availability of any electronic health information that is protected under the HIPAA Rules



Where is EPHI Found?

- Workstations
- Laptops
- Modems
- Databases
- Digitally recorded voice messages
- Computer-based facsimiles

- Servers
- Applications
- Network connections
- PDAs
- ***Biomedical devices***
- Compact disks
- Floppy diskettes

…..and many more!

Biomedical Devices

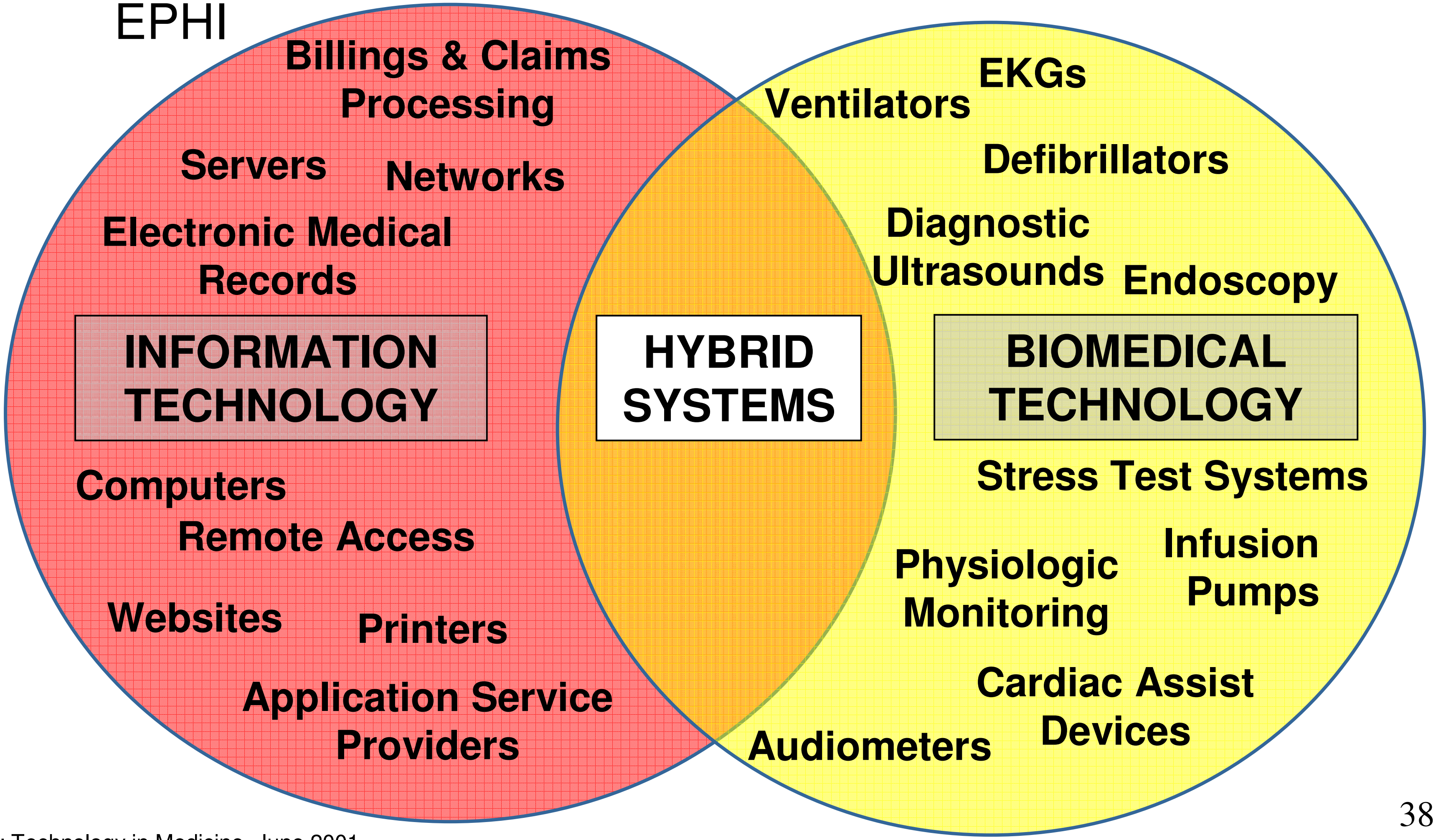
- A biomedical device is defined as “…an instrument which is intended for use in the diagnosis of disease, or other conditions, or in the cure, mitigation, treatment or prevention of disease…” (Food and Drug Administration, 1989)

- Majority of these instruments are highly automated and collect and store health information

HIPAA Security and Biomedical Devices

Systems

- Examples of devices/systems maintaining and transmitting EPHI

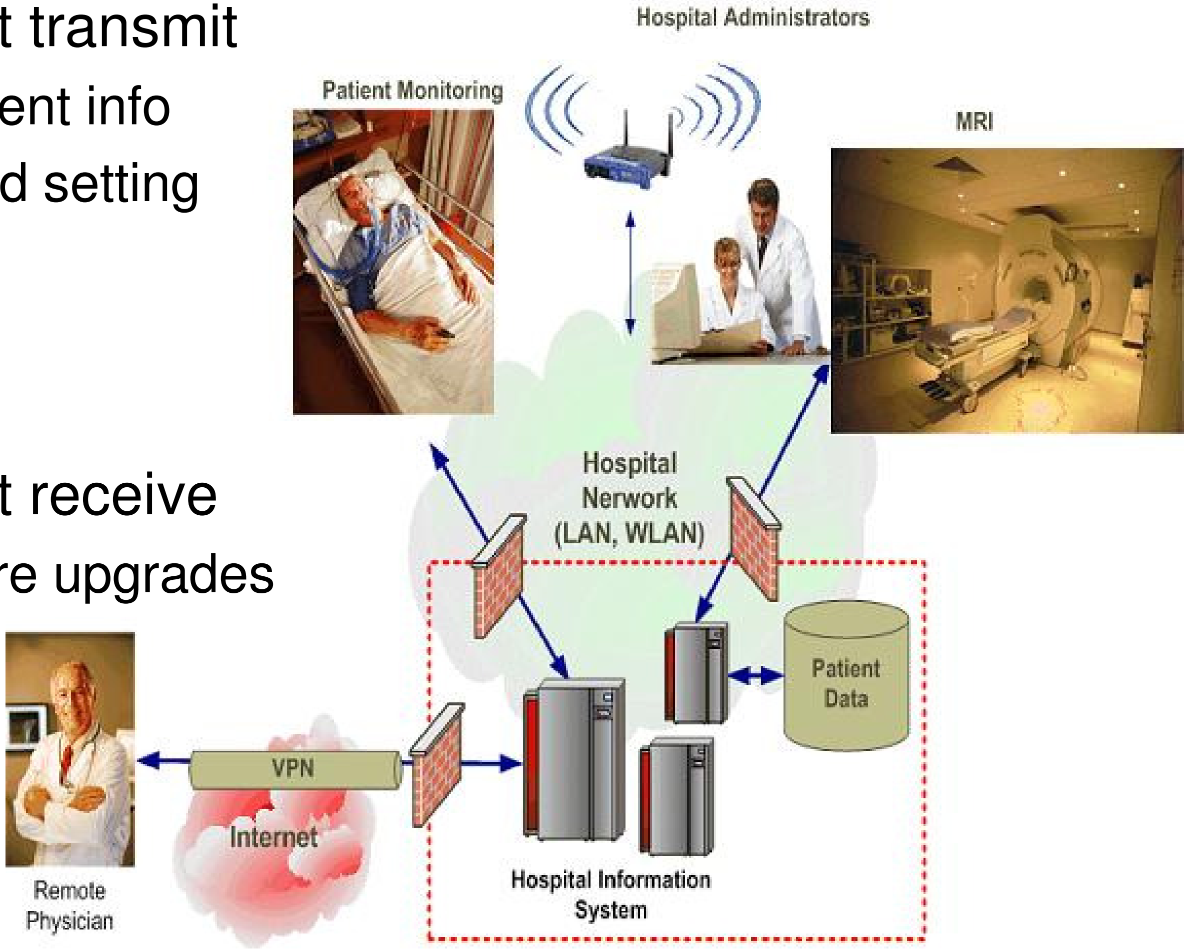


Source: Technology in Medicine, June 2001

HIPAA Security and Biomedical Devices

Biomedical Devices and IT Systems

- Devices on Internet transmit
  - Location and patient info
  - Current status and setting
  - Diagnostics
  - Error codes
- Devices on Internet receive
  - Software/Firmware upgrades
  - Calibration
  - Diagnostics



HIPAA Security and Biomedical Devices

Historical Perspective

- Biomedical devices utilized at MTFs operated either as stand-alone devices or as networked devices on isolated medical networks
- As such, biomedical devices with unresolved software vulnerabilities posed little or no security threat

HIPAA Security and Biomedical Devices

Current Perspective

- Potential threats
  - Migration of biomedical devices into interconnected networks
    - Subject to vulnerability alerts and patching requirements
  - Unresolved software vulnerabilities due to FDA regulations

HIPAA Security and Biomedical Devices

Security Risks (1 of 2)

- Biomedical devices
  - Frequently store EPHI, and therefore, must be considered when implementing a comprehensive IT security program
  - Designated and operated as special purpose computers
  - More features are being automated and increasing amounts of PHI is being collected, analyzed, and stored
  - Growing integration and interconnection of different biomedical devices and IT systems where EPHI is being exchanged

HIPAA Security and Biomedical Devices

Security Risks (2 of 2)

- “In its report covering security threats during the first quarter, McAfee's Anti-virus and Vulnerability Emergency Response Team (AVERT) said Monday that more than 1,000 new attacks aimed at software vulnerabilities emerged in the first three months of this year ” (CNET)
  - Blended threats continue to constitute the most frequently reported threat
    - Combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack

Issues

- FDA requires vendors of medical devices to evaluate the impact of software changes on a medical device's safety and effectiveness before installing a security patch or upgrade
  - Vendors do not include this type of repair and testing in standard maintenance agreement
  - Evaluation entails unanticipated costs and effort
    - Most computerized medical devices are non-compliant with these FDA requirements

HIPAA Security and Biomedical Devices

Impact: Organization

- **Risk assessment**
  - MTFs must evaluate the threat to and from biomedical devices in the context of their wider approach to risk management
- **Equipment lifecycle management**
  - Security requirements must be included in contracts or Memorandums of Understanding/Agreement
  - Evaluation and remediation of vulnerabilities must be conducted before the installation of devices on the network
- **Contracts**
  - Must accommodate need for security upgrades to relevant equipment as appropriate and affordable

HIPAA Security and Biomedical Devices

Impact: Architecture

- Multiple, overlapping controls must be developed to support Defense-in-Depth

- Biomedical devices that acquire, distribute, display and archive medical information should be placed on their own physical or virtual segment of the network

- Precise configuration of the medical enclave depends on architectural rules of the wider network

HIPAA Security and Biomedical Devices

Recommendations (1 of 2)

- Share information on solutions amongst your peers
  - FDA Guidance related to approved vendors
  - The impact is obvious – the more you share amongst your peers, the more time and resources you save
  - Information sharing should not be limited to individual Services but across the MHS

HIPAA Security and Biomedical Devices

Recommendations (2 of 2)

- Develop new requirements in vendor maintenance contracts to cover vulnerability alerts
  - Future contracts should require patches as a component of maintenance
  - Sit down with your vendor and agree on an approach to patching biomedical devices.

- **NOTE:** Precedence for vendors to accept this responsibility has not been established – this is especially true with legacy systems

Community Efforts to Address Issues

- Healthcare Information and Management Systems Society (HIMSS)
  - Biomedical Device Security Taskforce
    - http://www.himss.org/content/files/deviceSecurity/MDSBibliography.pdf
- National Electrical Manufactures Association (NEMA)
  - Joint Committee on Privacy and Security
    - http://www.nema.org/prod/med/security/
- NIST/WEDI/URAC
  - Biomedical Device Security Workgroup
    - http://www.urac.org/committees_sworkgroup.asp?navid=committees&pagename=committees_workgroups

HIPAA Security and Biomedical Devices

Summary

- You should now be able to:
  - Describe the relationship between HIPAA security and biomedical devices
  - Detail the risks of using biomedical devices
  - Identify approaches for minimizing these vulnerabilities

Training Summary

- You should now be able to:
  - Identify available resources to aide in Security Awareness
  - Identify available training briefings
  - Identify available resources to aide in implementation of HIPAA Security
  - Describe the relationship between HIPAA Security and biomedical devices

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm to subscribe to the TMA Privacy Office E-News
- Service HIPAA Security Representatives

Additional Resources

- RIMR
  - https://rimr.tatrc.org
- HIMSS
  - http://www.himss.org/content/files/deviceSecurity/MDSBibliography.pdf
- NEMA
  - http://www.nema.org/prod/med/security
- URAC
  - http://www.urac.org/committees_sworkgroup.asp?navid=committees&pagename=committees_workgroups

Please fill out your critique

Thanks!